## IN THE CLAIMS

	1. (cancelled)		
	2. (cancelled)		
1	3. (previously presented) The method as recited in claim 4, further comprising the		
2	step of:		
3	not unlocking the utility if the verifying step fails to verify the update to the		
4	utility.		
1	4. (previously presented) In a data processing system, a method for updating		
2	utility, comprising the steps of:		
3	receiving a request to unlock the utility;		
4	verifying an update to the utility;		
5	using a system management interrupt (SMI) handler to query a status of th		
6	verifying step; and		
7	if the verifying step successfully verifies the update of the utility, unlocking th		
8	utility and updating the utility, wherein the verifying step is performed by a trusted		
9	platform module (TPM) in accordance with Trusted Computing Platform Alliance		
10	Specifications.		
1	5. (original) The method as recited in claim 4, wherein the SMI handler used to		
2	query the status of the verifying step queries the TPM for the status.		
1	6. (currently amended) The method as recited in claim 5, In a data processing		
2	system, a method for updating a utility, comprising the steps of:		
3	receiving a request to unlock the utility;		
4	verifying an update to the utility;		
5	using a system management interrupt (SMI) handler to query a status of the		

6

verifying step; and

À				
7	if the verifying step successfully verifies the update of the utility, unlocking the			
8	utility and updating the utility, wherein the verifying step is performed by a trusted			
9	platform module (TPM) in accordance with Trusted Computing Platform Alliance			
10	Specifications, wherein the SMI handler used to query the status of the verifying step			
11	queries the TPM for the status, wherein the SMI handler is issued by the TPM.			
1	7.	(previously presented) The method as recited in claim 4, further comprising the		
2	step of:			
3	after the utility has been updated, locking the utility with the SMI handler.			
1	8.	(previously presented) The method as recited in claim 4, wherein the utility is a		
2	flash utility.			
1	9.	(previously presented) The method as recited in claim 4, wherein the requesting		
2	s performed by an SMI handler.			
	10.	(cancelled)		
	11.	(cancelled)		
1	12.	(previously presented) The computer program product as recited in claim 13,		
2	further comprising:			
3		programming for not unlocking the utility if the verifying programming fails to		
4	verify the update to the utility.			
1	13.	(previously presented) A computer program product for storage on a computer		
2	readal	ole medium and operable for updating a utility, comprising:		
3		programming for receiving a request to unlock the utility;		
4		programming for verifying an update to the utility;		

programming for verifying an update to the utility;

5

6

7

8

programming for using a system management interrupt (SMI) handler to query a status of the verifying programming; and

if the verifying programming successfully verifies the update of the utility, programming for unlocking the utility and updating the utility, wherein the verifying

9 programming is performed by a trusted platform module (TPM) in accordance with 10 Trusted Computing Platform Alliance Specifications. 1 14. (original) The computer program product as recited in claim 13, wherein the SMI 2 handler used to query the status of the verifying programming queries the TPM for the 3 status. 1 15. (original) The computer program product as recited in claim 14, wherein the SMI 2 handler is issued by the TPM. 1 16. (currently amended) The computer program product as recited in claim 13, further 2 comprising: 3 A computer program product for storage on a computer readable medium and 4 operable for updating a utility, comprising: 5 programming for receiving a request to unlock the utility; programming for verifying an update to the utility; 6 7 programming for using a system management interrupt (SMI) handler to query a 8 status of the verifying programming; 9 if the verifying programming successfully verifies the update of the utility, 10 programming for unlocking the utility and updating the utility, wherein the verifying 11 programming is performed by a trusted platform module (TPM) in accordance with 12 Trusted Computing Platform Alliance Specifications; and 13 after the utility has been updated, programming for locking the utility with the 14 SMI handler. 1 17. (previously presented) The computer program product as recited in claim 13, 2 wherein the requesting programming is performed by an SMI handler. 1 18. (original) A data processing system comprising: 2 a processor; 3 a trusted platform module (TPM) coupled to the processor and operating under

Trusted Computing Platform Alliance Specifications;

4

5	a BIOS utility stored in flash memory coupled to the processor;				
6	an input circuit for receiving an update to the BIOS utility; and				
7	a bus system for coupling the input circuit to the processor;				
8	a BIOS update application requesting an unlock of the flash memory from a				
9	system management interrupt (SMI) handler;				
10	the SMI handler including programming for requesting cryptographic verification				
11	of the BIOS utility update from the TPM;				
12	the TPM including programming for verifying an authenticity of the BIOS utility				
13	update;				
14	the TPM including programming for issuing an SMI to query the TPM for a status				
15	on the verifying of the authenticity of the BIOS utility update;				
16	the SMI handler unlocking the flash memory if the SMI handler sets the status as				
17	successful;				
18	the BIOS update application updating the BIOS utility with the update; and				
19	the SMI handler locking the flash memory after the update of the BIOS utility has				
20	completed.				
1	19. (original) A method comprising the steps of:				
2					
3	<ul> <li>(a) a BIOS update application requesting an unlock of a flash utility from</li> <li>a system management interrupt (SMI) handler;</li> </ul>				
4	(b) determining if a verification of an update to the flash utility is pending;				
5	(c) if verification of the update to the flash utility is not pending, the SMI				
6	handler requesting verification of the update to the flash utility from a trusted				
7	platform module (TPM) and setting a status flag as pending;				
8	(d) exiting the SMI handler and returning status flag to the BIOS update				
	• • • • • • • • • • • • • • • • • • • •				
12	(f) returning to step (a) if the status flag is set as pending after step (e);				
13	(g) in response to step (c), the TPM verifies the update to the flash utility;				
9 10 11	application;  (e) receiving by the BIOS update application the status flag from the SMI handler;				

14	(h)	when step (g) is completed, issuing an SMI by the TPM to query if the	
15	verification o	f the update to the flash utility was successful or failed;	
16	(i)	setting the status flag as successful if the verification of the update to	
17	the flash utility was successful;		
18	(j)	setting the status flag as failed if the verification of the update to the	
19	flash utility was not successful;		
20	(k)	if step (b) determines that verification of the update to the flash utility	
21	is still pending, determining if the verification of the update to the flash utility has		
22	completed;		
23	(1)	if step (k) determines that verification of the update to the flash utility	
24	has not completed, setting the status flag as pending;		
25	(m)	if step (k) determines that verification of the update to the flash utility	
26	has completed, determining if the verification of the update to the flash utility was		
27	successful;		
28	(n)	if step (m) determines that the verification of the update to the flash	
29	utility was no	t successful, setting the status flag as failed;	
30	(o)	if step (m) determines that the verification of the update to the flash	
31	utility was s	uccessful, the SMI handler unlocking the flash utility and setting the	
32	status flag as	successful;	
33	(p)	performing steps (d) and (e) in response to any of steps (l), (n), or (o);	
34	(q)	determining if the status flag is set as successful if after step (e) it is	
35	determined th	at the status flag is not set to pending; and	
36	(r)	updating the BIOS with the update to the flash utility and locking the	
37	flash utility	with the SMI handler if the status flag is determined to be set to	
38	successful in	step (q).	